§170.315(f)(1) Transmission to immunization registries

2015 Edition CCGs

Version 1.3 Updated on 06-15-2020

Revision History

Version #	Description of Change	Version Date
1.0	Initial Publication	10-29-2015
1.1	Updated the NIST Test Normative Test Process Document Link.	10-06-2016
1.2	Updated to include clarification to the CCG that compliance with the IG IM Release 1.5 addendum is required for testing and certification.	03-17-2017
1.3	Updated the Security requirements per 21st Century Cures Act.	06-15-2020

Regulation Text

Regulation Text

§170.315 (f)(1) *Transmission to immunization registries—*

(i) Create immunization information for electronic transmission in accordance with:
(A) The standard and applicable implementation specifications specified in §170.205(e)(4).
(B) At a minimum, the version of the standard specified in §170.207(e)(3) for historical vaccines.
(C) At a minimum, the version of the standard specified in §170.207(e)(4) for administered vaccines.

(ii) Enable a user to request, access, and display a patient's evaluated immunization history and the immunization forecast from an immunization registry in accordance with the standard at §170.205(e)(4).

Standard(s) Referenced

Paragraph (f)(1)(i)

§ 170.205(e)(4) HL7 2.5.1 *Implementation Specifications*. HL7 2.5.1 Implementation Guide for Immunization Messaging, Release 1.5, October 2014 and HL7 Version 2.5.1 Implementation Guide for Immunization Messaging (Release 1.5)—Addendum, July 2015

§ 170.207(e)(3) HL7 Standard Code Set CVX— Vaccines Administered, updates through August 17, 2015

§ 170.207(e)(4) National Drug Code (NDC) Directory– Vaccine NDC Linker, updates through August 17, 2015

Paragraph (f)(1)(ii)

§ 170.205(e)(4) HL7 2.5.1 *Implementation Specifications*. HL7 2.5.1 Implementation Guide for Immunization Messaging, Release 1.5, October 2014 and HL7 Version 2.5.1 Implementation Guide for Immunization Messaging (Release 1.5)—Addendum, July 2015

Certification Companion Guide: Transmission to immunization registries

This Certification Companion Guide (CCG) is an informative document designed to assist with health IT product development. The CCG is not a substitute for the 2015 Edition final regulation. It extracts key portions of the rule's preamble and includes subsequent clarifying interpretations. To access the full context of regulatory intent please consult the 2015 Edition final rule or other included regulatory reference. The CCG is for public use and should not be sold or redistributed.

Link to Final Rule Preamble

Edition Comparision	Gap Certification Eligible	Base EHR Definition	In Scope for CEHRT Definition
Revised	No	Not Included	Yes

Certification Requirements

Privacy and Security: This certification criterion was adopted at § 170.315(f)(1). As a result, an ONC-ACB must ensure that a product presented for certification to a § 170.315(f) "paragraph (f)" criterion includes the privacy and security criteria (adopted in § 170.315(d)) within the overall scope of the certificate issued to the product.

- The privacy and security criteria (adopted in § 170.315(d)) do not need to be explicitly tested with this specific paragraph (f) criterion unless it is the only criterion for which certification is requested.
- As a general rule, a product presented for certification only needs to be tested once to each applicable privacy and security criterion (adopted in § 170.315(d)) so long as the health IT developer

attests that such privacy and security capabilities apply to the full scope of capabilities included in the requested certification. However, exceptions exist for § 170.315(e)(1) "VDT" and (e)(2) "secure messaging," which are explicitly stated.
- § 170.315(d)(2)(i)(C) is not required if the scope of the Health IT Module does not have end-user device encryption features.

Table for Privacy and Security

- If choosing Approach 1:
  - Authentication, access control, and authorization (§ 170.315(d)(1))
  - Auditable events and tamper-resistance (§ 170.315(d)(2))
  - Audit reports (§ 170.315(d)(3))
  - End-user device encryption (§ 170.315(d)(7))
  - Encrypt authentication credentials (§ 170.315(d)(12))
  - Multi-factor authentication (MFA) (§ 170.315(d)(13))
- If choosing Approach 2:
  - For each applicable P&S certification criterion not certified for Approach 1, the health IT developer may certify using system documentation which is sufficiently detailed to enable integration such that the Health IT Module has implemented service interfaces the Health IT Module to access external services necessary to meet the requirements of the P&S certification criterion. Please see the *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program* Final Rule at 85 FR 25710 for additional clarification.

Design and Performance: The following design and performance certification criteria (adopted in § 170.315(g)) must also be certified in order for the product to be certified.
- When a single quality management system (QMS) is used, the QMS only needs to be identified once. Otherwise, the QMS' need to be identified for every capability to which it was applied.
- When a single accessibility-centered design standard is used, the standard only needs to be identified once. Otherwise, the accessibility-centered design standards need to be identified for every capability to which they were applied; or, alternatively the developer must state that no accessibility-centered design was used.

Table for Design and Performance

- Quality management system (§ 170.315(g)(4))
- Accessibility-centered design (§ 170.315(g)(5))

Technical Explanations and Clarifications

Applies to entire criterion

Clarifications:
- For the public health certification criteria in § 170.315(f), health IT will only need to be certified to those criteria that are required to meet the measures the provider intends to report on to meet Objective 8: Public Health and Clinical Data Registry Reporting.

- Any health IT can be certified to this criterion if it can meet all the requirements of the criterion, which include context exchange and vocabulary standards. There is no specified transport standard or mechanism required for this criterion. Consequently, any additional products used to facilitate immunization data submission in the manner required by the public health agency are not required to be included as part of Certified EHR Technology (CEHRT) implemented by eligible professionals, eligible hospitals, or critical access hospitals for those CMS programs requiring the use of CEHRT. Please consult CMS regulations for more specific requirements for meeting the CEHRT definition. [see also 80 FR 62663]
- While no transport standard is required for this criterion, an expert panel convened by the CDC and the American Immunization Registry Association (AIRA) has recommended a SOAP-based standard for transport of immunization data. Developers have the discretion to decide which transport standard(s) to implement. [see also 77 FR 54240]
- CDC issued an addendum to the HL7 2.5.1 Implementation Guide (IG) for Immunization Messaging (IM), Release 1.5. The addendum consolidates the IG IM Release 1.5 information that clarifies the conformance requirements, but does not specify additional substantive requirements. The addendum was adopted with the IG IM Release 1.5 for purposes of testing and certification to this criterion. [80 FR 62663]
- The criterion is not intended to specify when submissions should be made or the periodicity of the submissions. Consequently, submitting batch files to an immunization registry, provided that they are formatted according to the adopted standards referenced by this certification criterion, is not prohibited by this certification criterion and would be acceptable. [see also FAQ #2]
- The process for submitting immunization data often differs between public health agencies. We recommend developers work with the state or local immunization registry for guidance on how to submit the immunization data.
- We provide the following OIDs to assist developers in the proper identification and exchange of health information coded to certain vocabulary standards.
  - HL7 Standard Code Set CVX – Vaccine Administered OID: 2.16.840.1.113883.12.292
  - National Drug Code Directory OID: 2.16.840.1.113883.6.69 [80 FR 62612]
- Health IT Modules can present for certification to a more recent version of the CVX – Vaccines Administered and National Drug Code Directory – Vaccine Codes code sets than the August 17, 2015 updates per ONC's policy that permits certification to a more recent version of certain vocabulary standards. [80 FR 62620]

Paragraph (f)(1)(i)

Technical outcome – The Health IT Module can create immunization information according to the IG) IM Release 1.5, and the July 2015 Addendum, using CVX codes for historical vaccines and NDC codes for newly administered vaccines.

Clarifications:

- For the purposes of administered vaccines, when an immunization is reported at the time it is administered and the actual product is known, the NDC code must be sent. We clarify that for when sending historical vaccines and the actual NDC code is not available, CVX codes can be sent as this method would be supported by health IT certified to this criterion. [see also 80 FR 62663-62664]

Paragraph (f)(1)(ii)

Technical outcome – The Health IT Module enables a user to request, access and display the evaluated immunization history and forecast from an immunization registry for a patient in accordance with the HL7 2.5.1 standard, the HL7 2.5.1. IG for Immunization Messaging, Release 1.5, and July 2015 Addendum.

Clarifications:

- Health IT (e.g., EHR products) may sometimes have a version of the immunization history that differs from the history in the immunization registry. Likewise, Health IT (e.g., EHR products) that includes immunization forecasting capabilities may produce a forecast that differs from one produced by the immunization registry. We still believe that it is important for an EHR to receive the history and forecast from the registry. Based on compliance with the Release 1.5 IG, a user would be able to see and compare the history and forecast from the certified health IT (e.g., EHR product) with the history and forecast from the immunization registry. However, we note that this criterion does not prescribe a particular workflow or reconciliation requirements. Providers and health IT developers may reconcile forecast and history information in a manner that best meets their needs for workflow and patient safety. [see also 80 FR 62664]

Content last reviewed on June 23, 2020